

# How to Set Up a Secure Zoom Meeting

Updated 4/8/2020

## Overview and Simple Startup

If you need a video conferencing solution, consider Zoom, which allows you to host up to **100 attendees**. This would be great for a virtual Troop or Pack Meeting! Zoom also allows screen sharing, so you could have more than one leader in different locations running the meeting. Like Facebook Live and Skype, it's free to use and allows for you to quickly and easily share a virtual meeting with your Scouts.

How Do I Use Zoom?

Visit [zoom.us](https://zoom.us) and sign-in.

Click the "Host a Meeting" button at the top of your screen, choosing to have video on or off.

It will prompt you to join with computer audio, or you can click the check box to automatically join audio by computer when joining a meeting. You can also test your speaker and microphone.

Click the "Invite" button at the bottom of your screen and send an email OR copy the URL using the buttons on the "Invite people to join" pop-up window. Make note of the meeting password. Share your invitation and get started!

## Quick Start Zoom Settings

When setting up a Zoom meeting, there are logical and safety items that need to be addressed. I have colored all settings in **RED** or **BLUE**. **BLUE** is a suggestion; **RED** is mandatory for safe Zoom use. (These are not just for Zoom but for any presentation software like Google Meet, Google Hangouts, GoToMeeting, etc.)

1. **Optionally use the WAITING ROOM Feature** – This feature puts everyone in a waiting room and then you pick who should join your meeting.
2. **Use a PASSWORD** – Keep it simple but use it. It should be something all your scouts should remember like "grade2". No one can get in without this password. You will need to communicate this to all your scouts AND parents via email or text message.
3. **Turn off PRIVATE CHAT**. Group chat can be used, just not privately between scouts where you cannot monitor what's being said.
4. **Unless you need it for your meeting, turn off SCREEN SHARING**.
5. **Turn ON the "remove uninvited participant add "put participant on hold"**. By doing this you can kick anyone out of your meeting at any time.
6. **Do not post or join you link publicly. Do not put the link on your website. Email it to your scout AND parents.**
7. **LOCK your meeting once it has all your scouts.**
8. **Use practice sessions with your co-workers and try out the other features to see what you like and don't like. I am almost always able to get on you call.**
9. **Join your meeting at least 10 minutes before it's scheduled start. Early joiners will see that an adult is present, and the side conversations should stay much more scout appropriate.**

## Details and Security in a Zoom Meeting

With so many scouters using Zoom for virtual meetings, we wanted to remind you about “Zoom bombing” Zoom bombing is hijacking your meeting by someone outside your group. Here is a link with screen shots to show you how to change your Zoom settings and adjust your practices in order to protect your meetings from Zoom bombing: <https://www.pcmag.com/how-to/how-to-prevent-zoom-bombing>

### **How to Prevent Zoom-Bombing**

Zoom is becoming the videoconferencing method of choice during the COVID-19 pandemic. Unfortunately, your Zoom meetings are wide open to hijacking if you don't know how to set the host controls properly. Learn how to stop bad actors and keep your video calls on track.



Video calling app Zoom has seen a flood of activity recently, as people across the world shifted to remote work and schooling, due to novel coronavirus. More activity means more bad actors looking for vulnerabilities and other ways to exploit the app. That's how the term Zoom-bombing came to be. In a few instances of Zoom-bombing, according to a report from *Inside Higher Education*, [students exploited a screen sharing feature](#) that hadn't been locked by the instructor to put up pornographic and racist content for everyone on the call to see.

It wasn't a technological weakness in Zoom that allowed these events to occur. It was a matter of the host not knowing all the features of the tool and how to use them.

The best way to stop Zoom-bombing is to prevent it in the first place. When hosting a Zoom call, you need to set up your meeting, often in advance, using the right settings and features. (Beyond maintaining control of your meeting, there are other [Zoom tips](#) that will help you look like a Zoom pro.)

If you hastily launch a Zoom meeting and share the link publicly, it's much harder to stop trolls in the moment. Preventing a battle is better than having to fight one.

You can prevent Zoom-bombing with several simple tips and settings. Not every setting is available to free Zoom users, and when that's the case, there's a note at the top letting you know.

### 1. Use a Unique ID for Large or Public Zoom Calls

When you create a Zoom account, the app assigns you a Personal Meeting ID (PMI). It's a numeric code that you can give out to people when you want to meet with them. You can use it over and over; it doesn't expire. For standing meetings with a team or a weekly check-in, using the same code makes sense because people can join without having to hunt down this week's login number. It's always the same.

Zoom also gives you the option to *not* use your PMI for a meeting and instead generate a unique code. If you're the host of a large Zoom call where members of the public or other strangers are invited, it's much better to use a one-time code rather than your PMI. Here's why: Once you put your PMI into the world, people can use it to try and jump in on your Zoom calls at any time.

When you schedule a Zoom meeting, look for the Meeting ID options and choose Generate Automatically. Doing so plugs up one of the biggest holes that Zoom-bombers can exploit.

The image shows a screenshot of the Zoom 'Schedule Meeting' interface. The form is titled 'Schedule Meeting' and contains several sections for configuring a meeting. Two red arrows point to the 'Meeting ID' and 'Password' sections. The 'Meeting ID' section has two radio buttons: 'Generate Automatically' (which is selected) and 'Personal Meeting ID' (which is unselected). The 'Password' section has a checked checkbox for 'Require meeting password' and a text input field containing '08'. Other sections include 'Topic' (Jill Duffy's Zoom Chat), 'Date' (3/28/2020, 9:00 PM to 9:30 PM), 'Video' (Host and Participants both set to Off), 'Audio' (Telephone and Computer Audio selected), and 'Calendar' (Google Calendar selected). At the bottom, there are 'Cancel' and 'Schedule' buttons.

## 2. Require a Meeting Password

Let's say you publicly invite people to join a meeting, but you require an RSVP and are vetting the list of respondents. One way to protect the meeting is to require a password. That way, you can give the password out only to those who have replied and seem credible.

To password-protect a meeting, start by scheduling a meeting and checking the box next to Require meeting password. It's only an option when you generate a unique ID, not when you use your PMI.

You'll see a numeric password, which will work for everyone who has it.

## 3. Create a Waiting Room

A Zoom call can start one of two ways. It can start the moment the first person logs onto the call, or it can start when the host says it should start. For small groups of people who know each other, it's common for people to log in and make small talk while waiting for everyone else to join. Sometimes you want to let them chit-chat. For other calls, however, you might not want participants to chat with each other or even let the call officially start until you, the host, have signed in and are ready.

In that second case, the solution is to create a Zoom Waiting Room. When participants log into the call, they see a Waiting Room screen that you can customize, and they aren't let into the call until you, the host, lets them in. You can let people in all at once or one at a time, which means if you see names you don't recognize in the Waiting Room, you don't have to let them in at all.




## 4. Make Sure Only the Hosts Can Share Their Screen

Don't let anyone hijack the screen during a Zoom call. To prevent it, make sure your settings indicate that the only people allowed to share their screens are hosts.

You can enable this setting in advance as well as during a call.

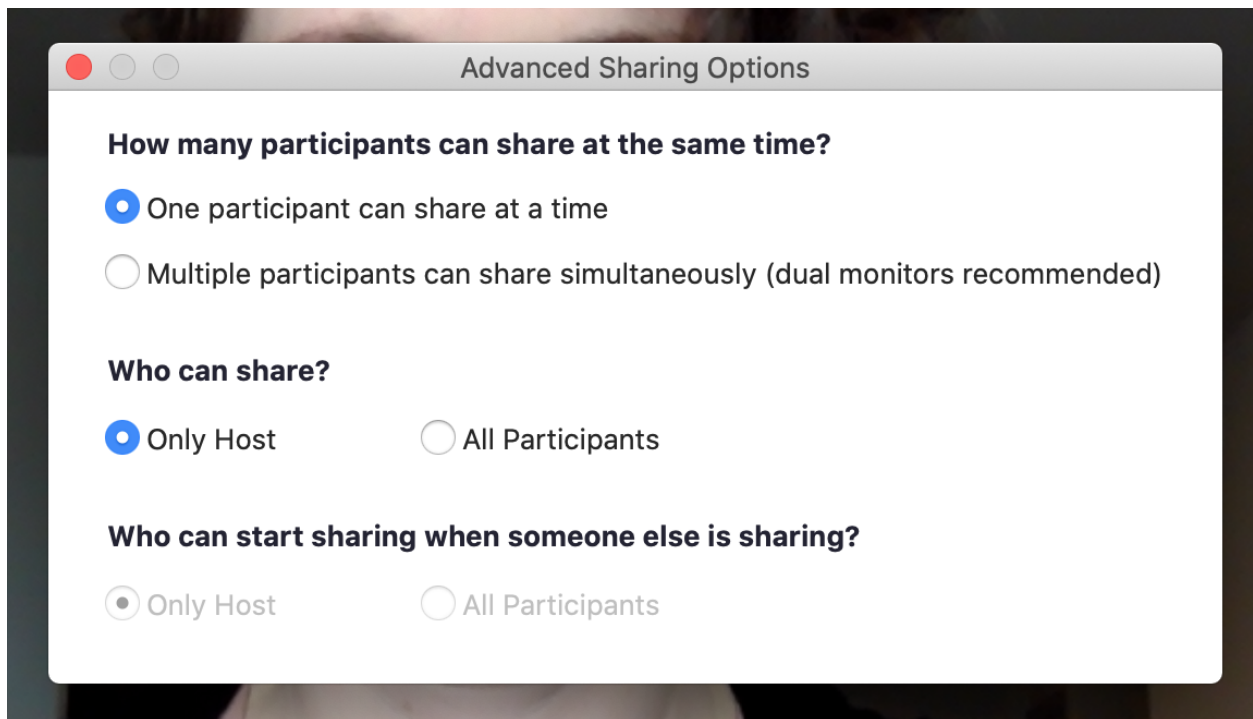
In advance, go to the Zoom web portal (not the desktop app) and in the settings navigate to Personal > Settings > In Meeting (Basic) and look for Screen sharing. Check the option that only the host can share.

---

Schedule Meeting	<b>Screen sharing</b> 
<b>In Meeting (Basic)</b>	Allow host and participants to share their screen or content during meetings
In Meeting (Advanced)	<b>Who can share?</b>
Email Notification	<input checked="" type="radio"/> Host Only <input type="radio"/> All Participants 
Other	<b>Who can start sharing when someone else is sharing?</b>
	<input checked="" type="radio"/> Host Only <input type="radio"/> All Participants 
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

During a call, you can prevent others from sharing their screens by using the host controls at the bottom. Click the up-facing carrot next to Share Screen. Choose Advanced Sharing Options and choose to only let the host

While sharing your screen or an image, Zoom has a great feature that lets participants annotate what they see. For visual collaboration, it's amazing. For naughty participants, it might seem like an invitation to bomb your call. You can disable the annotation feature in the In Meeting (Basics) section of your web account.



### 5. Create an Invite-Only Meeting

*This feature is for paid Zoom accounts only.*

One way to restrict who can join your Zoom call is to make it an invite-only meeting. That means the only people who can join the call are those you invited, and they must sign in using the same email address you used to invite them. It gives you much more assurance that people are who they say they are.

There are a few ways you can [enforce an invite-only meeting](#), depending on the type of account you have. The long and short of it is to look for an option called Authentication Profiles.

Once you have that setting enabled, anyone else who tries to join your meeting will see a notification on screen telling them that the meeting is for authorized attendees only.

## **6. Lock a Meeting Once It Starts**

If you start a meeting and everyone you expect to join has, you can lock the meeting from new participants. While the meeting is running, navigate to the bottom of the screen and click Manage Participants. The Participants panel will open. At the bottom, choose More > Lock Meeting.

## **7. Kick Someone Out or Put Them on Hold**

Sometimes an unruly participant manages to slip through the cracks. As the meeting host, you do have the power to kick someone out of a call or put them on hold.

**To kick someone out:** During the call, go to the participants pane on the right. Hover over the name of the person you want to boot and when options appear, choose Remove.

By default, an ousted guest cannot rejoin. What to do if you make a mistake? You can allow a booted party to rejoin. Enable this feature by going to the web portal and navigating to Settings > Meeting > In-Meeting (Basic). Toggle on the setting called Allow removed participants to rejoin.

### **RELATED**

[FBI: Watch Out for 'Zoom-Bombings' on Online Video Meeting Apps](#)  
[Students Conspire in Chats to 'Zoom-Bomb' Online Classes, Harass Teachers](#)  
[Top Zoom Tips for Better Videoconferencing in a Locked-Down World](#)

**To put someone on hold:** During the call, find the video thumbnail of the person you want to put on hold. I like to think of it as putting someone in a time-out. Click on their video image and select Start Attendee On Hold. Once they've learned their lesson, you can press Take Off Hold in the Participants panel.

## **8. Disable Someone's Camera**

Hosts can turn off any participant's camera. If someone is being rude or inappropriate on video, or their video has some technical problem, the host can open the Participants panel and click on the video camera icon next to the person's name.

## **9. Prevent Animated GIFs and Other Files in the Chat**

In the chat area of a Zoom meeting, participants can share files, including images and animated GIFs—if you let them. If you'd rather not, then be sure to disable file transfer. It's on by default, so you must actively disable it.

For your own meetings, open Settings in the Zoom web app (it's not in the desktop app). On the left side, go to Personal > Settings. Then click In Meeting (Basic). Scroll down a little farther until you see File Transfer. That's where you can disable it.

Schedule Meeting	<b>File transfer</b>	<input checked="" type="checkbox"/>
<a href="#">In Meeting (Basic)</a>	Hosts and participants can send files through the in-meeting chat. <input checked="" type="checkbox"/>	
In Meeting (Advanced)		
Email Notification	<b>Feedback to Zoom</b>	<input type="checkbox"/>
Other	Add a Feedback tab to the Windows Settings or Mac Preferences dialog, and also enable users to provide feedback to Zoom at the end of the meeting	

### 10. Disable Private Chat

If you're hosting a Zoom call and have invited strangers to join, someone in your crowd could harass another participant by sending them private messages. Or people could start talking behind your back. You can prevent this by disabling private chat. When you disable private chat, it doesn't affect the public chat, which everyone on the call can see and participate in.

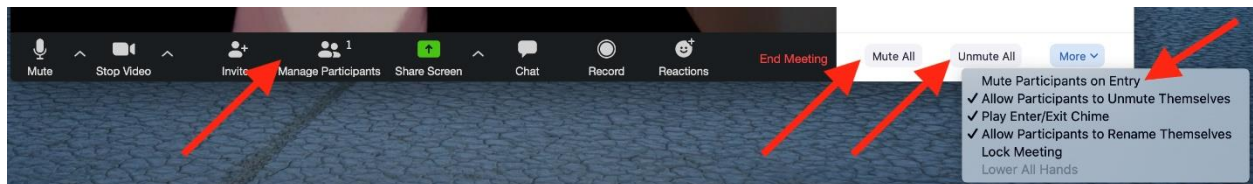
Schedule Meeting	<b>Chat</b>	<input checked="" type="checkbox"/>
<a href="#">In Meeting (Basic)</a>	Allow meeting participants to send a message visible to all participants	
In Meeting (Advanced)	<input type="checkbox"/> Prevent participants from saving chat <input checked="" type="checkbox"/>	
Email Notification	<b>Private chat</b>	<input type="checkbox"/>
Other	Allow meeting participants to send a private 1:1 message to another participant.	
	<b>Auto saving chats</b>	<input type="checkbox"/>
	Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.	

Open Settings in the Zoom web app (it's not in the desktop app). On the left side, go to Personal > Settings. Then click In Meeting (Basic). Scroll until you see Private chat. When the button is gray, it's disabled.

## ***Use These Additional Settings for Large Meetings***

Not all Zoom disruptors are bad actors. Sometimes participants make mistakes and don't realize that a yapping dog or crying child is causing a disturbance for everyone else. Or someone might accidentally upload a file they didn't mean to. Any time you host a meeting of more than one or two people, there are some settings in Zoom you should review and familiarize yourself with before the call.

**Mute participants.** Did you know the host can mute and unmute an individual or everyone on a call? While the call is ongoing, click Manage Participants at the bottom of the Zoom window. The participants panel opens, and you can individually mute people and disable their cameras by clicking the microphone or camera icon next to their name. The option to mute everyone at once is at the bottom of this pane.



**Mute upon entry.** You can also mute everyone automatically when they join a call. Before the call starts, go to the web portal and navigate to Settings > Meetings and choose the meeting. At the bottom of the screen, click to Edit the meeting. Look for Meeting Options and check the box next to Mute participants upon entry.

If you didn't set it up ahead of time, you can still mute people upon entry when you start the meeting. In the same panel shown above, look for the More option. Click it and choose Mute participants upon entry. You'll also see here an option to let participants unmute themselves. That's a useful setting if you want people to be able to speak up or ask questions at an appropriate time.

For further assistance on setting up a Zoom account please contact me at [markgaynor1112@gmail.com](mailto:markgaynor1112@gmail.com)

### ***Further Reading***

[How to Turn Your Smartphone Into a Wireless Webcam](#)

[Top Zoom Tips for Better Videoconferencing in a Locked-Down World](#)

[8 Tips for Better Video Conference Calls](#)

[10 Tips for Remote Job Interviews](#)

[More in How to Work From Home](#)

[More in Video Conferencing Software](#)

### ***Video Conferencing Software Reviews***

[Zoom Meeting](#)

[Microsoft Teams](#)

[Intermedia Unite](#)

[Cisco Webex Meetings](#)

[ClickMeeting](#)